Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Modernizing the E-rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	

Comments
OF
K-12 NATIONAL ADVISORY COUNCIL ON CYBERSECURITY

July 21, 2017

Table of Contents

I. INTRODUCTION & SUMMARY 3

II. THE COMMISSION SHOULD CONSIDER INCLUDING IN THE PROPOSED ELIGIBLE SERVICES LIST (ESL) SECURE GATEWAY PLATFORMS COMPRISED OF INTEGRATED ADVANCED THREAT DEFENSE TECHNOLOGY AS A NECESSARY REQUIREMENT TO MAKE CATEGORY ONE BROADBAND SERVICE FUNCTIONAL 5

III. CONCLUSION 7

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Modernizing the E-rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	

Comments
OF
K-12 NATIONAL ADVISORY COUNCIL ON CYBERSECURITY

1. INTRODUCTION & SUMMARY

The Executive Board of the K-12 National Advisory Council on Cybersecurity (K-12 NACC) agrees with the Wireline Competition Bureau FY2016 order and petitions the Commission to include Secure Web Gateway network capabilities including: *Intrusion Prevention (IPS), Intrusion Detection (IDS), Virus Protection, Data Leakage Protection (DLP),* to make Category One broadband service functional. Millions of students across the U.S. are connecting to unprotected broadband services - jeopardizing their online safety and the integrity and reliability of public schools local and wide area networks (LAN/WAN). Considering cyberthreats, transported via broadband services are successfully and increasingly penetrating public schools and district LAN/WAN's; compromising millions of student records including social security numbers and student safety online, the K-12 NACC believes the lack of fundamental cybersecurity protections associated with broadband services, is contributing

directly to the inability of U.S. public education institutions to comply with Federal mandates, including the Family Educational Rights and Privacy Act (FERPA).

The K-12 NACC; a public entity (www.NACCedu.org) with a mission to ensure public education institutions across the nation have the tools and information needed to ensure advanced cyber threat protections for their networks, student information systems, and resources, and expert guidance and thought leadership associated with the adoption of practical cybersecurity strategies and recommended best-of-breed solutions, hereby submits these comments in response to the June 21, 2017 public notice released by the Wireline Competition Bureau ("Bureau") in the above – captioned proceedings. The Public Notice seeks comment for the FY2018 ESL regarding the FY2016 ESL order, whereby the Wireline Competition Bureau found that equipment is eligible for Category One support if it is "necessary to make a Category One broadband service functional".

Therefore, in consideration of the direct correlation between the growing requirement for K-12 broadband connectivity; (consistent with the 2010 National Educational Technology Plan, and the former administrations ConnectED initiative, which calls for connecting 99 percent of America's students to the internet through high-speed broadband and high-speed wireless within five years), and the growing documented impact cyberattacks are inflicting by directly impeding and/or contaminating broadband data streams connecting to public schools, data systems and students accessing educational resources via the internet, we believe now is the time to include

these fundamental capabilities in to the FY2018 ESL. Hence, the K-12 NACC vigorously petitions the Commission to include Secure Web Gateway network capabilities including: *Intrusion Prevention (IPS), Intrusion Detection (IDS), Virus Protection, Data Leakage Protection (DLP),* in to the FY2018 ESL order.

II. THE COMMISSION SHOULD INCLUDE IN THE FY2018 ELIGIBLE SERVICES LIST (ESL) SECURE GATEWAY PLATFORMS COMPRISED OF INTEGRATED ADVANCED THREAT DEFENSE TECHNOLOGY, AS A NECESSARY REQUIREMENT TO MAKE CATEGORY ONE BROADBAND SERVICE FUNCTIONAL

The Consortium for School Networking (CoSN) 2016 Annual Infrastructure Survey indicated for a second year in a row that more students have access to non-shared devices; either provided by the school or through a Bring Your Own Device (BYOD) program. 38 percent of school systems reported that 100 percent of students have access to non-shared devices at high school compared to 36 percent in middle school and 18 percent in elementary school. This is a significant increase from 2015 when 25 percent of school systems reported that 100 percent of students have access to non-shared devices at high school and middle school. Each of those thousands of students must connect directly to the public school/districts LAN/WAN on and off the school premises, to gain access to broadband services currently unprotected. Additionally, all systems and applications connecting to the school network; who serve as the custodian for millions of student records via Student Information and Learning Management systems (SIS/LMS), are also profoundly compromised.

Lack of Secure Web Gateway network security associated with broadband services has contributed directly to Cybersecurity attacks impacting schools and districts with increasing frequency. Distributed Denial of Service (DDoS) attacks, in which outside systems overwhelm

the bandwidth and resources of a targeted system, have made headlines for disrupting online testing. Data breaches, whether caused by human error, theft, or hacking pose great financial and legal risks for schools, and often result in identity theft, impacting student's and school employees. Malware, ransomware, and social engineering attacks are crippling school networks and compromise student and employee data, resulting in significant and costly disruption to school operations and breaches to Federal mandates.

These growing threats could be mostly mitigated if a public school/districts broadband services would include Secure Web Gateway network capabilities verses relying on traditional Firewalls and Unified Threat Management Systems, (UTM's) which fail to provide the required protections to secure school networks connecting to broadband services. Traditional Firewalls do not offer security to client endpoints surfing the Internet. Firewalls are configured to allow users to access the Internet, but do not control which websites users visit or what content (including viruses and malware) the client downloads from those websites. UTM's offer blended security capabilities, but most have evolved from traditional firewalls, and offer significant limitations including:

1. When advanced security capabilities such as Secure Socket Layer (SSL) inspection are enabled, performance drops significantly, causing administrators to choose between performance/usability and security – *most IT staff forgo security*.
2. UTM's can inspect data streams, however cannot terminate Transmission Control Protocols (TCP) sessions, including proxy, producing a reactionary verses proactive security posture.

3. UTM's do not have the ability to inspect webpage/file content, secure network gateways do – providing significantly more proactive/behavioral security capabilities associated with inbound and outbound broadband data streams.

The CoSN 2016 Infrastructure Survey confirms most school systems see an increasing need for broadband access, with 75 percent projecting they'll experience increases in demand for Internet access in the next 18 months. More than a quarter of respondents — 27 percent — indicated the increase will be 100 percent to 499 percent above current demand, and another four percent indicated demand would skyrocket to 500 percent within 18 months. Driving that demand are:

1. More students with devices;
2. Online assessments (the No. 1 driver for rural schools);
3. Digital content (the No. 2 driver for urban and rural schools);
4. More devices per student;
5. Mobile learning

III. CONCLUSION

In direct contrast to the increasing dependency on broadband connectivity, the U.S. Department of Education has confirmed that nearly 50 percent of all public districts surveyed in 2016 reported spending less than four percent of their technology budget on cybersecurity. Almost 20 percent of schools and districts reported spending less than one percent. Only 42 percent of school and district technology leaders believe their organizations take a proactive or very proactive approach to addressing cybersecurity.

In a 2015 Verizon Data Breach Investigations Report, public education was ranked the number two U.S. target of hackers. Cybersecurity attacks represent a real and significant threat to the integrity of broadband services connecting to public education networks. The analogy of constructing a super highway with questionable infrastructure integrity - safeguards and proactive protection, applies when considering the millions of students at risk and the responsibility public officials have to comply with Federal mandates, ensure students safety online, and keep their data privacy protected. The K-12 NACC therefore supports the Commissions FY2016 order, as such respectfully requests the Wireline Bureau act to ensure broadband services are not compromised by adding Web Gateway network capabilities to the FY2018 ESL.

Respectfully Submitted,

By: /s/ Ronald S. Chandler
Ronald S. Chandler
Chair, K-12 National Advisory Council on Cybersecurity